

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-014441

(43)Date of publication of application : 19.01.2001

(51)Int.Cl.

G06K 19/073

G06F 12/14

G06K 17/00

H04L 9/32

(21)Application number : 11-374788

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 28.12.1999

(72)Inventor : HIROTA TERUTO
TATEBAYASHI MAKOTO
YUGAWA YASUHEI
MINAMI MASANAO
KOZUKA MASAYUKI

(30)Priority

Priority number : 11119441

Priority date : 27.04.1999

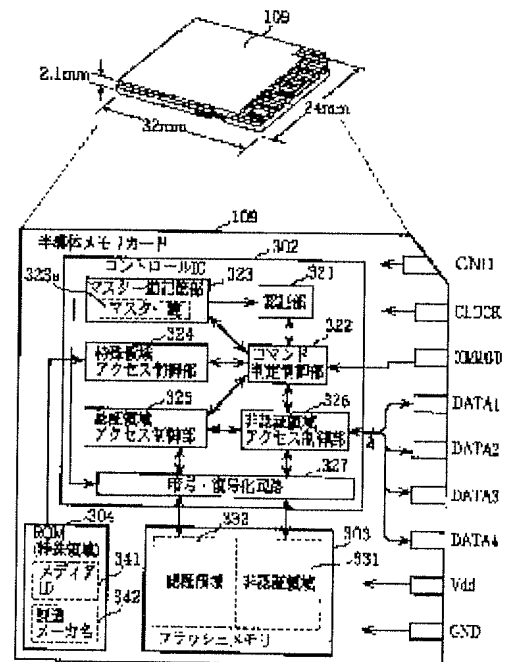
Priority country : JP

(54) SEMICONDUCTOR MEMORY CARD AND READER

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a semiconductor memory card usable as a storage medium for digital literary works and also usable as a storage medium for general computer data (non-literary works) for which the protection of copyright is not required.

SOLUTION: This card is composed of a control IC 302, a flash memory 303 and a ROM 304, the ROM 304 holds a medium ID 341 or the like peculiar to this card, the flash memory 303 has an authentication area 332 for permitting access to external equipment only when the authentication of that external equipment is made successful and a non-authentication area 331 for permitting access regardless of the authenticated result and the control IC 302 has control parts 325 and 326 for controlling access from the external equipment to the authentication area 332 and the non-authentication area 331 and an authentication part 321 or the like for executing mutual authentication with the external equipment.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-14441

(P2001-14441A)

(43) 公開日 平成13年1月19日 (2001.1.19)

(51) Int.Cl.⁷

識別記号

F I

デコード* (参考)

G 0 6 K 19/073

G 0 6 K 19/00

P 5 B 0 1 7

G 0 6 F 12/14

3 2 0

G 0 6 F 12/14

3 2 0 A 5 B 0 3 5

G 0 6 K 17/00

G 0 6 K 17/00

E 5 B 0 5 8

H 0 4 L 9/32

H 0 4 L 9/00

6 7 5 A 5 J 1 0 4

6 7 5 D

審査請求 未請求 請求項の数17 O L (全 27 頁)

(21) 出願番号

特願平11-374788

(22) 出願日

平成11年12月28日 (1999.12.28)

(31) 優先権主張番号

特願平11-119441

(32) 優先日

平成11年4月27日 (1999.4.27)

(33) 優先権主張国

日本 (J P)

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 廣田 照人

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(72) 発明者 館林 誠

大阪府門真市大字門真1006番地 松下電器

産業株式会社内

(74) 代理人 100090446

弁理士 中島 司朗 (外1名)

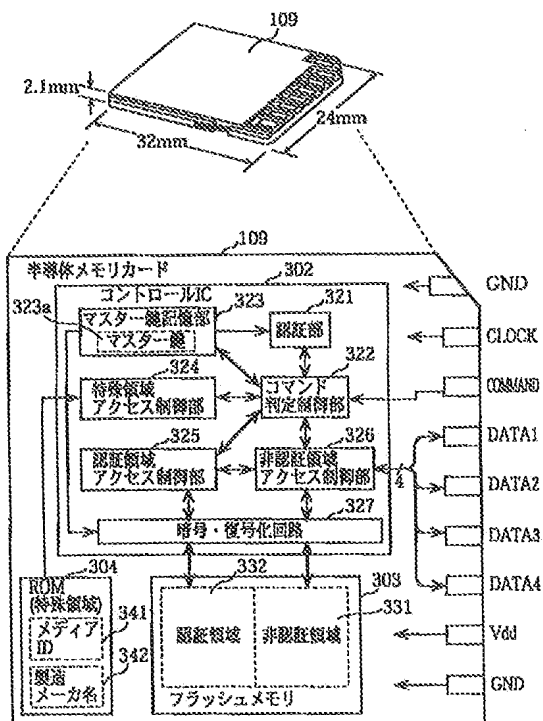
最終頁に続く

(54) 【発明の名称】 半導体メモリカード及び読み出し装置

(57) 【要約】

【課題】 デジタル著作物の記憶媒体として用いることが可能であり、かつ、著作権保護が必要とされない一般的なコンピュータデータ（非著作物）の記憶媒体としても用いることが可能な半導体メモリカードを提供する。

【解決手段】 コントロールIC302とフラッシュメモリ303とROM304とからなり、ROM304は、このカードに固有のメディアID341等を保持し、フラッシュメモリ303は、外部機器の認証に成功した場合にのみその外部機器にアクセスを許可する認証領域332と認証の結果に拘わらずアクセスを許可する非認証領域331とを有し、コントロールIC302は、外部機器による認証領域332及び非認証領域331へのアクセスを制御する制御部325、326及び外部機器との相互認証を実行する認証部321等を有する。



と物理アドレスとの対応を示す変換テーブルと、前記電子機器からの命令に従って前記変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御することを特徴とする請求項1記載の半導体メモリカード。

【請求項13】 前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項14】 前記不揮発メモリは、フラッシュメモリであり、前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有することを特徴とする請求項1記載の半導体メモリカード。

【請求項15】 前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有することを特徴とする請求項1記載の半導体メモリカード。

【請求項16】 請求項1記載の半導体メモリカードに格納されたデジタル著作物を読み出す読み出し装置であって、前記半導体メモリカードは、非認証領域に、デジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の読み出しを許可する回数が予め格納され、前記読み出し装置は、前記非認証領域に格納されたデジタル著作物を読み出す際に、前記認証領域に格納された回数を読み出し、その回数によって読み出しが許可されているか否か判断する判断手段と、許可されている場合にのみ前記非認証領域から前記デジタル著作物を読み出すとともに、読み出した前記回数を減算して前記認証領域に書き戻す再生手段とを備えることを特徴とする読み出し装置。

【請求項17】 請求項1記載の半導体メモリカードに

格納されたデジタル著作物を読み出してアナログ信号に再生する読み出し装置であって、前記半導体メモリカードは、非認証領域に、アナログ信号に再生可能なデジタル著作物が格納されているとともに、認証領域に、前記デジタル著作物の前記電子機器によるデジタル出力を許可する回数が予め格納され、前記読み出し装置、前記非認証領域に格納されたデジタル著作物を読み出してアナログ信号に再生する再生手段と、前記認証領域に格納された回数を読み出し、その回数によってデジタル出力が許可されているか否か判断する判断手段と、許可されている場合にのみ前記デジタル著作物をデジタル信号のまま外部に出力するとともに、読み出した前記回数を減算して前記認証領域に書き戻すデジタル出力手段とを備えることを特徴とする読み出し装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、デジタル著作物等を記憶するための半導体メモリカード及びその読み出し装置に関し、特に、デジタル著作物の著作権保護に好適な半導体メモリカード及び読み出し装置に関する。

【0002】

【従来の技術】 近年、マルチメディア・ネットワーク技術の発展により、音楽コンテンツ等のデジタル著作物がインターネット等の通信ネットワークを通じて配信されるようになり、自宅に居ながらにして世界中の音楽等に接することが可能となってきた。例えば、パーソナルコンピュータ（以下、「PC」という。）で音楽コンテンツをダウンロードした後、PCに装着された半導体メモリカードに格納しておくことで、必要に応じて音楽を再生し楽しむことができる。また、このようにして音楽コンテンツを格納した半導体メモリカードをPCから取り出して携帯型音楽再生装置に装着しておくことで、歩きながら音楽を聴くこともできる。このような半導体メモリカードは、フラッシュメモリ等の不揮発性で、かつ、大きな記憶容量の半導体メモリを内蔵した小型軽量の便利なカードである。

【0003】 ところで、このような電子音楽配信において、半導体メモリカードにデジタル著作物を記憶する場合、不正なコピーを防止するために、鍵等を用いてコンテンツを暗号化しておく必要がある。また、PC等に標準添付されて広く出回っているファイル管理ソフトウェアによっては他の記憶媒体等にコピーすることができないようにしておく必要もある。

【0004】 このような不正なコピーを防止する方法として、半導体メモリカードへのアクセスを専用のソフトウェアでのみ可能とする方策が考えられる。例えば、PCと半導体メモリカード間での認証が成功した時にのみ半導体メモリカードへのアクセスを許可することとし、

き込みが許可されている場合には、そのアプリケーションは、暗号化された音楽データ、パスワード、権利情報をメモリカード109に書き込むことができる。図2は、このメモリカード109を記録媒体とする携帯型の録音再生装置（以下、「プレーヤ」という。）201の外観を示す図である。

【0015】プレーヤ201の上面には、液晶表示部203と操作ボタン202が設けられ、手前側面には、メモリカード109を着脱するためのメモリカード挿入口206及びPC102等と接続するためのUSB等の通信ポート213が設けられ、右側面には、アナログ出力端子204、デジタル出力端子205及びアナログ入力端子223等が設けられている。

【0016】プレーヤ201は、メモリカード109に格納された音楽データ、パスワード、権利情報に基づいて、再生が許可されている状態にあるならば、その音楽データを読み出して復号した後にアナログ信号に変換し、アナログ出力端子204に接続されたヘッドフォン208を通じて音声として出力したり、再生中の音楽データをデジタルデータのままデジタル出力端子205に出力したりする。

【0017】また、このプレーヤ201は、マイク等を介してアナログ入力端子223から入力されるアナログの音声信号をデジタルデータに変換してメモリカード109に記録したり、通信ポート213を介して接続されたPC102と通信することによって、そのPC102によってダウンロードされた音楽データ、パスワード及び権利情報をメモリカード109に記録することができる。つまり、このプレーヤ201は、メモリカード109への音楽データの記録及びメモリカード109に記録された音楽データの再生に関して、図1に示されたPC102及びメモリカードライタ107に置き換わる機能を有する。

【0018】図3は、PC102のハードウェア構成を示すブロック図である。PC102は、CPU110、デバイス鍵111aや制御プログラム111b等を予め記憶しているROM111、RAM112、ディスプレイ103、通信回線101と接続するためのモデムポートやプレーヤ201と接続するためのUSB等を備える通信ポート113、キーボード104、内部バス114、メモリカード109と内部バス214とを接続するメモリカードライタ107、メモリカード109から読み出された暗号化音楽データを復号するデスクランブラ1117、復号された音楽データを伸張するMPEG2-AAC（ISO13818-7）に準拠したAACデコーダ118、伸張されたデジタル音楽データをアナログ音声信号に変換するD/Aコンバータ119、スピーカ106及びファイル管理ソフトウェアやアプリケーションを格納しているハードディスク120等から構成される。

【0019】このPC102は、ハードディスク120に格納されたファイル管理ソフトウェアを実行することで、メモリカード109をハードディスクのように独立したファイルシステム（ISO9293等）を有する補助記憶装置として用いることができるだけでなく、ハードディスク120に格納された上述の専用アプリケーションを実行することで、通信ポート113のモデム等を介して通信回線101から音楽コンテンツ等をダウンロードしたり、メモリカード109との相互認証を行なった後に音楽コンテンツ等をメモリカード109に格納したり、メモリカード109に格納されている音楽コンテンツ等を読み出してスピーカ106に再生出力したりする。

【0020】なお、ROM111に格納されたデバイス鍵111aは、このPC102に固有の秘密鍵であり、後述するように、相互認証等に用いられる。図4は、プレーヤ201のハードウェア構成を示すブロック図である。プレーヤ201は、CPU210、デバイス鍵211aや制御プログラム211b等を予め記憶しているROM211、RAM212、液晶表示部203、PC102等と接続するためのUSB等の通信ポート213、操作ボタン202、内部バス214、メモリカード109と内部バス214とを接続するカードI/F部215、メモリカード109との相互認証を実行する認証回路216、メモリカード109から読み出された暗号化音楽データを復号するデスクランブラ217、復号された音楽データ伸張するMPEG2-AAC（ISO13818-7）に準拠したAACデコーダ218、伸張されたデジタル音楽データをアナログ音声信号に変換するD/Aコンバータ219、スピーカ224、アナログ入力端子223から入力されたアナログ音楽信号をデジタル音楽データに変換をするA/Dコンバータ221、そのデジタル音楽データをMPEG2-AAC（ISO13818-7）に準拠して圧縮符号化するAACエンコーダ220、圧縮符号化された音楽データを暗号化するスクランブラ222、アナログ出力端子204、デジタル出力端子205及びアナログ入力端子223から構成される。

【0021】このプレーヤ201は、ROM211に格納された制御プログラム211bをRAM212にロードしCPU210に実行させることで、メモリカード109に格納されている音楽コンテンツ等を読み出してスピーカ224に再生出力したり、アナログ入力端子223や通信ポート213を経て入力された音楽コンテンツ等をメモリカード109に格納したりする。つまり、通常のプレーヤと同様に、個人的に音楽を録音したり再生したりして楽しむことができるだけでなく、PC102によりダウンロードされた電子音楽配信に係る（著作権保護が必要とされる）音楽コンテンツの記録・再生もできる。

む際にそのデータを暗号化して書き込み、フラッシュメモリ303からデータを読み出した際にそのデータを復号化する。これは、不正なユーザがこのメモ리카ード109を分解してフラッシュメモリ303の内容を直接解析し、認証領域332に格納されたパスワードを盗む等の不正行為を防止するためである。

【0031】なお、コントロールIC302は、これら主要な構成要素321～327の他に、クロックピンから供給されるクロック信号に同期した内部クロック信号を生成し各構成要素に供給する同期回路や、揮発性の記憶領域及び不揮発性の記憶領域等を有する。また、特殊領域(ROM304)に格納されている情報の改ざんを防止するために、そのROM304をコントロールIC302の中に内蔵させたり、それらの情報をフラッシュメモリ303に格納し、外部から書き込みできないように特殊領域アクセス制御部324が制限をかけてもよい。そのときに、暗号・復号化回路327で暗号化したデータを格納することとしてもよい。

【0032】図6は、PC102やプレーヤ201から見たメモ리카ード109の記憶領域の種類を示す図である。メモ리카ード109が有する記憶領域は、大きく分けて、特殊領域304と認証領域332と非認証領域331の3つの領域である。特殊領域304は読み出し専用の領域で、この中のデータに対しては、専用コマンドを用いて読み出しを行う。認証領域332は、PC102又はプレーヤ201とメモ리카ード109との間で認証が成功した時にのみ読み書きができる領域で、この領域へのアクセスについては暗号化されたコマンドを用いる。非認証領域331は、ATAやSCSI等の公開されたコマンドでアクセスできる、即ち、認証せずに読み書きできる領域である。従って、非認証領域331に対しては、フラッシュATAやコンパクトフラッシュと同じように、PC102上のファイル管理ソフトウェアでデータの読み書きが可能である。

【0033】3つの記憶領域には、以下の情報を格納することとし、これによって、一般的なPCの補助記憶装置として機能と、電子音楽配信に係る音楽データに対する著作権保護の機能とを提供している。つまり、非認証領域331には、著作権保護の対象となる音楽データが暗号化された暗号化コンテンツ426や、著作権保護とは無関係な一般的なデータであるユーザデータ427等が格納される。認証領域332には、非認証領域331に格納された暗号化コンテンツ426を復号するための秘密鍵となる暗号化キー425が格納される。そして、特殊領域304には、認証領域332にアクセスするために必要とされる情報であるメディアID341が格納されている。

【0034】PC102やプレーヤ201は、まず、装着されたメモ리카ード109の特殊領域304に格納されたメディアID341を読み出し、それを用いて認証

領域332に格納された暗号化キー425、権利情報を取り出す。それら暗号化キー425や権利情報によって再生が許可されていれば、非認証領域331にある暗号化コンテンツ426を読み出し、暗号化キー425で復号しながら、再生を行うことができる。

【0035】もし、あるユーザが不正に入手した音楽データだけをPC102等でメモ리카ード109の非認証領域331に書き込み、そのようなメモ리카ード109をプレーヤ201に装着して再生しようとしたとする。しかし、そのメモ리카ード109の非認証領域331に音楽データが格納されているものの、認証領域332に対応する暗号化キー425や権利情報が存在しないために、そのプレーヤ201は、その音楽データを再生することができない。これによって、正規の暗号化キーや権利情報を伴わないで音楽コンテンツだけをメモ리카ード109に複製しても、その音楽コンテンツは再生されないの、デジタル著作物の不正な複製が防止される。

【0036】図7は、PC102やプレーヤ201がメモ리카ード109の各領域にアクセスする際の制限やコマンドの形態を示す図であり、(a)は各領域へのアクセスにおけるルールを示し、(b)は各領域のサイズの変更におけるルールを示し、(c)はメモ리카ード109の領域を示す概念図である。特殊領域304は、読み出し専用の領域であり、認証せずに専用コマンドでアクセスできる。この特殊領域304に格納されたメディアID341は、認証領域332にアクセスするための暗号化コマンドの生成や復号に用いられる。つまり、PC102やプレーヤ201は、このメディアID341を読み出し、これを用いて認証領域332にアクセスするコマンドを暗号化し、メモ리카ード109に送る。一方、その暗号化コマンドを受けたメモ리카ード109は、メディアID341を用いて、その暗号化コマンドを復号し、解釈して実行する。

【0037】認証領域332は、PC102やプレーヤ201等のメモ리카ード109にアクセスする装置とメモ리카ード109との間で認証が成功した時にのみアクセスが可能となる領域であり、その大きさは(YYYY+1)個のセクタに相当する。つまり、この認証領域332は、論理的には、第0～YYYYのセクタで構成され、物理的には、フラッシュメモリ303の第XXXX～第(XXXX+YYYY)のセクタアドレスを有するセクタから構成される。なお、セクタアドレスとは、フラッシュメモリ303を構成する全てのセクタそれぞれに対してユニークに付された一連の番号のことである。

【0038】非認証領域331は、認証せずにATAやSCSI等の標準コマンドでアクセスすることが可能で、その大きさはXXXX個のセクタに相当する。つまり、この非認証領域331は、論理的にも物理的にも第0～(XXXX-1)のセクタで構成される。なお、フラッシュメモリ303には、認証領域332や非認証領

10

20

30

40

50

25)の読み出しに先立ち、認証領域332から読み出すためのコマンドを暗号化してメモ리카ード109に送信しておく。

(4)得られた暗号化キー425をマスター鍵323aとメディアID341で復号化し、パスワードを抽出する(S705)。このときの復号化は、図8に示されたステップS605での暗号化の逆変換である。

【0050】(5)最後に、非認証領域331から暗号化コンテンツ426を読み出し、上記ステップS705で抽出したパスワードで復号しながら音楽を再生していく(S706)。このように、メモ리카ード109の非認証領域331に格納された音楽データは、認証領域332の暗号化キー425がないと復号することができない。従って、たとえ不正に音楽データだけを別のメモ리카ードにコピーしたとしても、その音楽データを正常に再生することができないので、その音楽データの著作権は安全に保護される。

【0051】また、認証に成功した機器だけがメモ리카ードの認証領域へのアクセスが許可されるので、認証に用いられるデバイス鍵や暗号化アルゴリズム等を適切に選択して用いることで、一定の条件を満たした機器だけに対してメモ리카ードの認証領域へのアクセスを許可する等の著作権保護が可能となる。なお、この例では、メモ리카ード109に暗号化コンテンツを記録する際に、その暗号化に用いられたパスワードをマスター鍵とメディアIDで暗号化し、暗号化キーとして認証領域332に格納されたが(S605)、マスター鍵及びメディアIDのいずれかを用いて暗号化することとしてもよい。これによって、暗号の強度が低下する恐れがあるものの、暗号化の簡略化に伴い、メモ리카ード109やプレーヤ201等の回路規模が小さくなるという利点を得られる。

【0052】また、プレーヤ201やPC102は、認証により、メモ리카ード109からマスター鍵323aを取り出したが、予めプレーヤ201やPC102にそのマスター鍵323aを埋め込んでおいてもよいし、マスター鍵323aを暗号化し、暗号化マスター鍵として特殊領域304に格納しておいてもよい。次に、このようなメモ리카ードの認証領域の活用例として、「読み出し回数」を格納した例と、「デジタル出力許可回数」を格納した例を示す。

【0053】図10は、プレーヤ201(及びPC102)がメモ리카ード109の認証領域に格納された読み出し回数812を操作する動作を示すフロー図である。ここでは、メモ리카ード109に格納された読み出し回数812の範囲内でのみ、プレーヤ201が、メモ리카ード109の非認証領域331に格納された音楽データを音声信号に再生することが許可されている場合(S801)について説明する。

【0054】(1)プレーヤ201は、デバイス鍵21

1a等を用いて、メモ리카ード109の認証部321とチャレンジ・レスポンス型の認証を行い、その認証に成功すると、まず、メモ리카ード109からマスター鍵323aを取り出す(S802)。

(2)次に、専用コマンドを用いて、メモ리카ード109の特殊領域304に格納されているメディアID341を取り出す(S803)。

【0055】(3)続いて、メモ리카ード109の認証領域332から音楽データの暗号化キー425を取り出す(S704)。このときには、データ(暗号化キー425)の読み出しに先立ち、認証領域332から読み出すためのコマンドを暗号化してメモ리카ード109に送信しておく。

(4)次に、メモ리카ード109の認証領域332から読み出し回数812を取り出し、その値を検査する(S804)。その結果、その値が無制限な読み出しを許可する旨の値である場合は、図9に示された手順(S704~S706)と同様の手順に従って、音楽を再生する(S806~S808)。

【0056】(5)一方、読み出し回数812が0を示す場合は、もはや再生が許可されていないと判定し(S805)、再生処理を終了する(S809)。そうでない場合は、その読み出し回数812を1つ減算し、その結果を認証領域332に書き戻した後に(S805)、上記手順に従って、音楽を再生する(S806~S808)。

【0057】このように、メモ리카ード109の認証領域332に、予め許可された再生回数を指定した読み出し回数812を格納しておくことにより、プレーヤ201による音楽再生の回数をコントロールすることが可能となる。これによって、例えば、レンタルCDやKIOSK端末等によるアナログ再生に適用することが可能となる。

【0058】なお、読み出し回数812に代えて、「読み出し時間」とすることで、音楽コンテンツを再生することが可能な総時間を制限することもできる。また、回数と時間とを組み合わせてもよい。さらに、読み出し回数812は、再生を開始してから10秒等の一定時間を超えて再生され続けた場合にだけ、その回数を減算してもよい。また、読み出し回数812は、不正な改ざんを防ぐために暗号化して格納することとしてもよい。

【0059】図11は、プレーヤ201(及びPC102)がメモ리카ード109の認証領域に格納されたデジタル出力許可回数913を操作する動作を示すフロー図である。ここでは、メモ리카ード109に格納されたデジタル出力許可回数913の範囲内でのみ、プレーヤ201が、メモ리카ード109の非認証領域331に格納された音楽データを読み出してデジタル出力することが許可されている場合(S901)について説明する。

【0060】(1)プレーヤ201は、図9に示された

ンター値としてPC102等に送る(S1002)。

【0070】(2)取得したカウンタ値と、既に取得しているマスター鍵323a及びメディアID341とからパスワードを生成する(S1003)。

(3)書き込むべき1セクタ分のデータをパスワードで暗号化しながら、メモリカード109に送る(S1004)。このとき、書き込むべきセクタを指定する情報や、暗号化に用いたカウンタ値も一緒に送る

(4)メモリカード109は、受け取った暗号化データを、指定されたセクタ1004に書き込む(S1006)。

【0071】(5)その暗号化データからECCを計算し、上記セクタに対応する拡張領域1005に、ECCデータ1006として書き込む(S1007)。

(6)続いて、上記暗号化データとともに受け取ったカウンタ値を時変領域1007に書き込む(S1008)。次に、PC102がメモリカード109からデータを読み出す場合(S1011)の手順を説明する。

【0072】(1)PC102は、メモリカード109に対して、セクタを指定するとともにデータの読み出しを要求する。すると、メモリカード109は、まず、指定されたセクタ1004の暗号化データだけを読み出してPC102に出力し(S1016)、PC102は、その暗号化データを受け取る(S1012)。

(2)次に、メモリカード109は、指定されたセクタ1004に対応する拡張領域1005の時変領域1007に格納されたカウンタ値を読み出してPC102に出力し(S1017)、PC102は、そのカウンタ値を受け取る(S1013)。

【0073】(3)読み出したカウンタ値と、既に取得しているマスター鍵323a及びメディアID341とからパスワードを生成する(S1014)。

(4)そのパスワードを用いて、暗号化データを復号する(S1015)。ここで、もし、不正な改ざん等により、セクタ1004のデータが変更されている場合には、時変領域1007から読み出されたカウンタ値との不整合が生じ、元のデータに復元されない。

【0074】このように、フラッシュメモリ303内に、ユーザからは見えない(アクセスできない)隠し領域としての時変領域1007を設け、そこに格納されたカウンタ値に依存したパスワードでデータを暗号化し格納することで、不正なユーザによるデータの改ざんを防止することができる。なお、ここでは、時変領域1007は、ECCを格納するための拡張領域1005としたが、メモリカードの外部から書き換えができない領域であれば、フラッシュメモリ303内の他の領域に設けてもよい。

【0075】また、カウンタ値は、乱数であったが、刻々と変化する時刻等のタイマー値としたり、フラッシュメモリ303への書き込み回数を示す値としてもよ

い。次に、フラッシュメモリ303の論理アドレスと物理アドレスとの対応づけについて、好ましい例を説明する。図13は、論理アドレスと物理アドレスとの対応を変更する様子を示す図であり、(a)は変更前の対応関係、(b)は変更後の対応関係、(c)は(a)に対応する変換テーブル1101、(d)は(b)に対応する変換テーブル1101を示す。

【0076】ここで、変換テーブル1101は、全ての論理アドレス(ここでは、論理ブロックの番号)と各論理アドレスに対応する物理アドレス(ここでは、フラッシュメモリ303を構成する物理ブロックの番号)とを組にして記憶するテーブルであり、コントロールIC302内の不揮発な記憶領域等に保存され、認証領域アクセス制御部325や非認証領域アクセス制御部326によって論理アドレスを物理アドレスに変換する際等において参照される。

【0077】メモリカード109にアクセスする機器は、メモリカード109中の物理的に存在するすべてのデータ空間(フラッシュメモリ303を構成する全ての物理ブロック)にデータを書き込めるのではなく、論理アドレスによって特定できる論理的なデータ空間(論理ブロック)にのみデータを書き込むことができる。この理由の一つは、フラッシュメモリ303の一部が破損し読み書きが行えなくなった場合に、その領域を置き換えるための代替領域を確保しておかなければならないからである。そして、そのような欠陥ブロックを代替領域中のブロックと置き換えた場合であっても、その対応づけの変更を変換テーブルに反映しておくことで、複数の連続する物理ブロックからなるファイルの論理的な連続性は維持されるので、外部機器に対しては破損が生じなかったように見せかけることができる。

【0078】ところが、複数のブロックからなるファイル等をメモリカード109に格納したり、削除したりすることを繰り返していると、論理ブロックのフラグメンテーションが増大する。つまり、図13(a)に示されるように、同一のファイルfile1を構成する論理ブロックであるにも拘わらず、それらの論理アドレスが不連続となってしまう。

【0079】これでは、例えば、音楽データをメモリカード109に格納しようとしたときに、メモリカード109の論理的な連続領域に書けないので、各ブロック毎に書き込みコマンド「Write address count」を発行する必要がある、書き込み速度が低下してしまう。同様に、読み出し動作においても、1曲を構成する音楽データであるにも拘わらず、各ブロック毎に読み出しコマンド「Read address count」を発行する必要がある、音楽データのリアルタイム再生が困難となってしまう。

【0080】この問題を解決する方法として、このメモリカード109のコントロールIC302は、外部機器からのコマンドに基づいて、変換テーブル1101を書

ブロック（ここでは、物理ブロック 4 と 5）を特定した後（ステップ S 1 2 0 3）、メモリカード 1 0 9 に対して、それらブロック 4 と 5 の番号を指定した消去コマンドを発行する（ステップ S 1 2 0 4）。そのコマンドを受信したメモリカード 1 0 9 のコマンド判定制御部 3 2 2 は、アクセス制御部 3 2 5、3 2 6 に指示を出す等により、指定された物理ブロック 4 と 5 を一括消去する。

【0 0 9 1】これによって、もし、その物理ブロック 4 と 5 への書き込みが発生した場合には、その物理ブロックに対する消去処理は不要となるので、高速な書き込みが可能となる。次に、このメモリカード 1 0 9 が有する個人データの保護に関する機能、具体的には、メモリカード 1 0 9 が外部機器を認証する際にその外部機器を使用するユーザの個人データを必要とする場合における個人データの保護機能について説明する。ここで、個人データとは、そのユーザを一意に識別するためのデータであって、メモリカード 1 0 9 の認証領域 3 3 2 へのアクセスが許可された正規のユーザとしてメモリカード 1 0 9 に識別させるためのデータである。

【0 0 9 2】このような場合において、認証領域 3 3 2 へのアクセスの度にユーザに対して繰り返し個人データを入力することを要求したり、その個人データを認証領域 3 3 2 に格納することとしたのでは、不正者によって盗聴されたり、認証領域 3 3 2 にアクセスする権限を有する他のユーザによって見られたりする不都合がある。

【0 0 9 3】これを防止するために、音楽データと同様に、個人データについても、個人が設定したパスワードで暗号化してから格納するという方法が考えられる。しかしながら、パスワードを設定した場合には、その個人データを見るたびにパスワードを入力しなければならず、手続が面倒であり、その管理も必要となる。そこで、このメモリカード 1 0 9 は、不必要に個人データを繰り返し入力することを回避する機能を有する。

【0 0 9 4】図 1 5 は、認証のためのプレーヤ 2 0 1 とメモリカード 1 0 9 間の通信シーケンス及び主要な構成要素を示す図である。なお、本図に示される処理は、主にプレーヤ 2 0 1 の認証回路 2 1 6 及びメモリカード 1 0 9 の認証部 3 2 1 によって実現される。本図に示されるように、プレーヤ 2 0 1 の認証回路 2 1 6 は、暗号化及び復号化等の機能の他に、メモリカード 1 0 9 に保持されたマスター鍵 3 2 3 a と同一の秘密鍵であるマスター鍵 1 3 0 1 と、製造番号 (s/n) 等のプレーヤ 2 0 1 に固有の ID である機器固有 ID 1 3 0 2 とを予め記憶している。

【0 0 9 5】また、メモリカード 1 0 9 の認証部 3 2 1 は、暗号化、復号化及び比較等の機能に他に、2 つの不揮発な記憶領域である機器固有 ID 群記憶領域 1 3 1 0 とユーザキー記憶領域 1 3 1 1 とを有する。機器固有 ID 群記憶領域 1 3 1 0 は、このメモリカード 1 0 9 の認

証領域 3 3 2 へのアクセスが許可された全ての機器の機器固有 ID を記憶しておくための記憶領域であり、ユーザキー記憶領域 1 3 1 1 は、個人データとして機器から送られてきたユーザキーを記憶しておくための記憶領域である。

【0 0 9 6】具体的な認証手順は、以下の通りである。なお、送受信においては、全てのデータは暗号化されて送信され、受信側で復号される。そして、手順が進む度に、次の手順での暗号化及び復号化に用いられる鍵が生成される。

(1) メモリカード 1 0 9 とプレーヤ 2 0 1 とを接続すると、まず、プレーヤ 2 0 1 は、マスター鍵 1 3 0 1 を用いて機器固有 ID 1 3 0 2 を暗号化し、メモリカード 1 0 9 に送る。

【0 0 9 7】(2) メモリカード 1 0 9 は、受け取った暗号化された機器固有 ID 1 3 0 2 をマスター鍵 3 2 3 a で復号し、得られた機器固有 ID 1 3 0 2 が既に機器固有 ID 群記憶領域 1 3 1 0 に格納されているか検査する。

(3) その結果、既に機器固有 ID 1 3 0 2 が格納されている場合は、認証が成功した旨をプレーヤ 2 0 1 に通知し、一方、機器固有 ID 1 3 0 2 が格納されていない場合は、プレーヤ 2 0 1 に対しユーザキーを要求する。

【0 0 9 8】(4) プレーヤ 2 0 1 は、ユーザキーの入力をユーザに促した後に、ユーザから個人データとしてのユーザキーを取得し、そのユーザキーをメモリカード 1 0 9 に送る。

(5) メモリカード 1 0 9 は、送られてきたユーザキーと予めユーザキー記憶領域 1 3 1 1 に格納されているものとを比較し、一致している場合、又は、ユーザキー記憶領域 1 3 1 1 が空であった場合は、認証が成功した旨をプレーヤ 2 0 1 に通知するとともに、上記ステップ

(3) で獲得した機器固有 ID 1 3 0 2 を機器固有 ID 群記憶領域 1 3 1 0 へ格納する。

【0 0 9 9】これによって、ユーザが所有する機器とメモリカード 1 0 9 とを初めて接続した場合は個人データ（ユーザキー）の入力が必要とされるが、2 回目以降においては、その機器の機器固有 ID が用いられて自動的に認証が成功するので、再び、個人データの入力を要求されることはない。次に、本メモリカード 1 0 9 と P C 1 0 2 やプレーヤ 2 0 1 等の外部機器との認証プロトコルの変形例について、図 1 6 及び図 1 7 を用いて説明する。

【0 1 0 0】図 1 6 は、変形例に係るメモリカード 1 0 9 と外部機器（ここでは、プレーヤ 2 0 1）との認証手順を示す通信シーケンス図である。ここでの処理は、主に、変形例に係るプレーヤ 2 0 1 の認証回路 2 1 6、P C 1 0 2 の制御プログラム 1 1 1 b 及びメモリカード 1 0 9 の認証部 3 2 1 によって実現される。また、メモリカード 1 0 9 のマスター鍵記憶部 3 2 3 には、暗号化さ

ンスデータと、チャレンジデータとして送った乱数を暗号化して得られる暗号化チャレンジデータとを比較し、一致している場合には、メモリカード109の認証に成功した(OK)と認識し、そのメモリカード109の認証領域332へのアクセスコを行う。一方、比較の結果、一致しなかった場合には、認証に成功しなかった(NG)したと認識し、そのメモリカード109の認証領域332へのアクセスは断念する。

【0110】なお、これら相互認証における暗号化アルゴリズムは、メモリカード109及びプレーヤ201が正当な機器である限り、全て同一である。また、メモリカード109及びプレーヤ201は、それぞれの認証及び証明において生成した暗号化チャレンジデータとレスポンスデータとを排他的論理和演算し、得られた結果をセキュア鍵として、メモリカード109の認証領域332へのアクセスのために用いる。そうすることで、双方の機器109及び201が相互認証に成功した場合のみ共通となり、かつ、時変のセキュア鍵を共有し合うことが可能となり、これによって、認証領域332にアクセスする条件として相互認証に成功していることが条件とされることになる。

【0111】なお、セキュア鍵の生成方法として、暗号化チャレンジデータとレスポンスデータとセキュアメディアIDとの排他的論理和をとることとしてもよい。次に、本メモリカード109の認証領域332と非認証領域331との境界線の変更機能についての変形例について、図18及び図19を用いて説明する。図18は、境界線を変更する前のフラッシュメモリ303の使用状態を示す図である。図18(a)は、フラッシュメモリ303の物理ブロックの構成を示すメモリマップである。

【0112】図18(b)は、非認証領域アクセス制御部326内の不揮発な記憶領域等に置かれる非認証領域331専用の変換テーブル1103であり、非認証領域331の論理ブロックと物理ブロックとの対応関係が格納されている。非認証領域アクセス制御部326は、この変換テーブル1103を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【0113】図18(c)は、認証領域アクセス制御部325内の不揮発な記憶領域等に置かれる認証領域332専用の変換テーブル1102であり、認証領域332の論理ブロックと物理ブロックとの対応関係が格納されている。認証領域アクセス制御部325は、この変換テーブル1102を参照することで、論理アドレスを物理アドレスに変換したり、割り当て領域を越えるアクセス違反を検出することができる。

【0114】境界線の変更前においては、図18(a)に示されるように、フラッシュメモリ303の代替領域を除いた記憶領域(物理ブロック0000~EFFF)のうち、境界線よりも下位アドレスに位置する物理ブ

ック0000~DFFFが非認証領域331に割り当てられ、上位アドレスに位置する物理ブロックE000~EFFFが認証領域332に割り当てられている。

【0115】そして、図18(b)に示された変換テーブル1102から分かるように、非認証領域331においては、物理ブロックと論理ブロックの番号が一致するように対応づけられている。一方、図18(c)に示された変換テーブル1103から分かるように、認証領域332においては、物理ブロックと論理ブロックとは、その番号の並びが逆順になっている。つまり、論理ブロック0000~0FFFそれぞれが物理ブロックEFFF~E000に対応している。これは、論理ブロックは昇順に使用されていくことと、境界線が移動された場合において領域変更の生じた物理ブロックのデータ退避や移動処理の手間を考慮したからである。

【0116】図19(a)~(c)は、境界線を変更した後のフラッシュメモリ303の使用状態を示す図であり、それぞれ、変更前の図18(a)~(c)に対応する。なお、境界線の変更は、そのアドレスを指定する専用のコマンドがコマンドピンからコマンド判定制御部322に入力されたときに、コマンド判定制御部322によって認証領域アクセス制御部325内の変換テーブル1102及び非認証領域331内の変換テーブル1103が書き換えられることにより、実現される。

【0117】図19(a)~(c)に示されるように、ここでは、物理ブロックE000とDFFF間に置かれていた境界線が物理ブロックD000とCFFF間に移動されている。つまり、非認証領域331のサイズを1000(hex)個だけ減少させ、認証領域332のサイズを1000(hex)だけ増加させている。それに伴って、図19(b)に示されるように、非認証領域331の変換テーブル1103のサイズは、1000(hex)個のエントリー分だけ減少され、その結果、論理ブロック0000~CFFFに対応する物理ブロック0000~CFFFが示されている。一方、図19(c)に示されるように、認証領域332の変換テーブル1102のサイズは、1000(hex)個のエントリー分だけ増加され、その結果、論理ブロック0000~1FFFに対応する物理ブロックEFFF~D000が示されている。

【0118】このように、フラッシュメモリ303の一定領域において境界線によって非認証領域と認証領域とを区切り、その境界線の移動によって各領域のサイズを変更することにより、このメモリカード109の多様な応用、例えば、保護すべきデジタル著作物の格納を主要な用途とする場合やその逆の場合等に対応させることが可能となる。

【0119】そして、非認証領域及び認証領域いずれにおいても、境界線に近いアドレスの物理ブロックから境界線に近いアドレスの物理ブロックに向かって、使用し

ズ変更回路は、前記一定サイズの記憶領域を2分する境界アドレスを変更することによって前記認証領域及び前記非認証領域それぞれの領域サイズを変更するとしてもよい。これによって、境界線を移動させるだけで認証領域及び非認証領域の領域サイズを変更することができるので、そのための回路は小さくて済む。

【0130】また、前記領域サイズ変更回路は、前記認証領域における論理アドレスと物理アドレスとの対応を示す認証領域変換テーブルと、前記非認証領域における論理アドレスと物理アドレスとの対応を示す非認証領域変換テーブルと、前記電子機器からの命令に従って前記認証領域変換テーブル及び前記非認証領域変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部は、前記認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御し、前記非認証領域アクセス制御部は、前記非認証領域変換テーブルに基づいて前記電子機器によるアクセスを制御するとしてもよい。

【0131】これによって、認証領域と非認証領域で、変換テーブルが独立分離されているので、それぞれの領域サイズや論理アドレスと物理アドレスとの対応を個別に管理することが容易となる。また、前記認証領域及び前記非認証領域は、それぞれ、前記一定サイズの記憶領域を2分して得られる物理アドレスの高い領域及び低い領域に割り当てられ、前記非認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの昇順となるように論理アドレスと物理アドレスとが対応づけられ、前記認証領域変換テーブルは、論理アドレスの昇順が物理アドレスの降順となるように論理アドレスと物理アドレスとが対応づけられているとしてもよい。

【0132】これによって、論理アドレスの昇順に使用していくことで、認証領域と非認証領域との境界付近の領域が使用される確立が低くなるので、その境界を移動させた場合に必要とされるデータ回避や移動等の処理が発生する確率も低くなり、領域サイズの変更が簡単化される。また、前記半導体メモリカードはさらに、予めデータが格納された読み出し専用のメモリ回路を備えてもよい。これによって、他の半導体メモリカードと区別できる識別データ等を読み出し専用メモリに格納し、デジタル著作物をその識別データに依存させて格納したりすることで、著作権保護の機能が強化される。

【0133】また、前記認証領域及び前記非認証領域は、前記電子機器にとって読み書き可能な記憶領域と読み出し専用の記憶領域とからなり、前記制御回路はさらに、前記電子機器が前記不揮発メモリにデータを書き込むためのアクセスをする度に乱数を発生する乱数発生器を有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記乱数を用いて前記データを暗号化し、得られた暗号化データを前記読み書き可能な記憶領域に書き込むとともに、前記乱数を前記暗号化デー

タに対応づけられた前記読み出し専用の記憶領域に書き込むとしてもよい。

【0134】これによって、読み書き可能な記憶領域に対する不正な改ざん等が行われても、読み出し専用の記憶領域に格納された乱数との整合性を検査することで、そのような行為を検出することが可能となるので、より安全なデータ記録が実現される。また、前記制御回路はさらに、前記認証領域及び前記非認証領域における論理アドレスと物理アドレスとの対応を示す変換テーブルと、前記電子機器からの命令に従って前記変換テーブルを変更する変換テーブル変更部とを有し、前記認証領域アクセス制御部及び前記非認証領域アクセス制御部は、前記変換テーブルに基づいて前記電子機器によるアクセスを制御するとしてもよい。

【0135】これによって、同一ファイルを構成する複数の論理ブロックが断片化する現象が生じて、論理的に連続した論理ブロックとなるように容易に変更することができるので、同一ファイルへのアクセスが高速化される。また、前記制御回路はさらに、前記認証領域及び前記非認証領域に書き込むべきデータを暗号化するとともに、前記認証領域及び前記非認証領域から読み出されたデータを復号化する暗号復号部を有してもよい。これによって、半導体メモリカードを破壊して認証領域及び非認証領域のメモリ内容を直接読み出す等の不正な攻撃に耐えることが可能となる。

【0136】また、前記不揮発メモリは、フラッシュメモリであり、前記制御回路はさらに、前記電子機器からの命令に従って、前記認証領域及び前記非認証領域に存在する未消去の領域を特定し、その領域を示す情報を前記電子機器に送る未消去リスト読み出し部を有してもよい。これによって、電子機器は、フラッシュメモリの書き換えに先立って、未消去の領域を知り、その領域を事前に消去しておくことができるので、高速な書き換えが可能となる。

【0137】また、前記認証部は、認証のために電子機器を使用するユーザに対してそのユーザに固有の情報であるユーザキーを要求するものであり、前記制御回路はさらに、前記ユーザキーを記憶しておくためのユーザキー記憶部と、前記認証部による認証に成功した電子機器を特定することができる識別情報を記憶しておくための識別情報記憶部と、前記認証部による認証が開始されると、その電子機器から識別情報を取得し、その識別情報が前記識別情報記憶部に既に格納されているか否か検査し、既に格納されている場合には、前記認証部によるユーザキーの要求を禁止させるユーザキー要求禁止部とを有してもよい。

【0138】これによって、半導体メモリカードと接続して使用する度にパスワードや個人データの入力が必要とされるという手間が回避されるので、不正に個人データが盗聴されて利用されるという不具合の発生が抑えられ

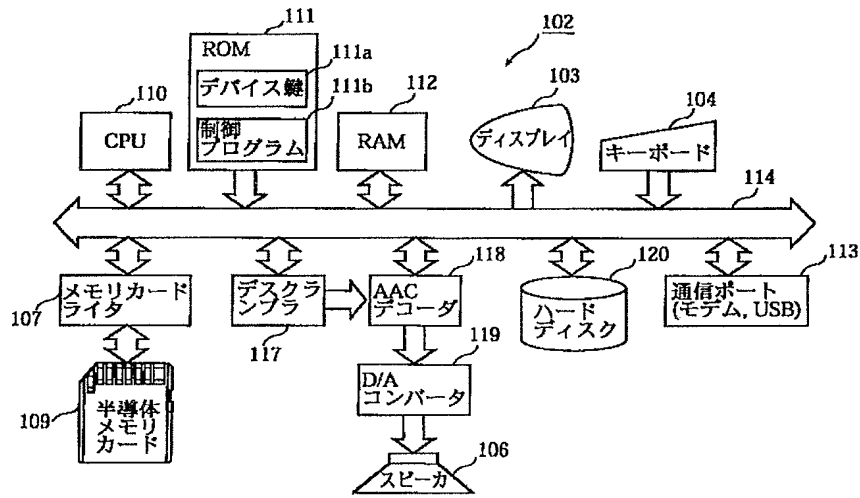
換テーブルを示し、(c)は認証領域専用の変換テーブルを示す。

【図19】同半導体メモリカードの認証領域と非認証領域との境界線の変更における変更後の状態を示す図であり、(a)はフラッシュメモリの物理ブロックの構成を示すメモリマップであり、(b)は非認証領域専用の変換テーブルを示し、(c)は認証領域専用の変換テーブルを示す。

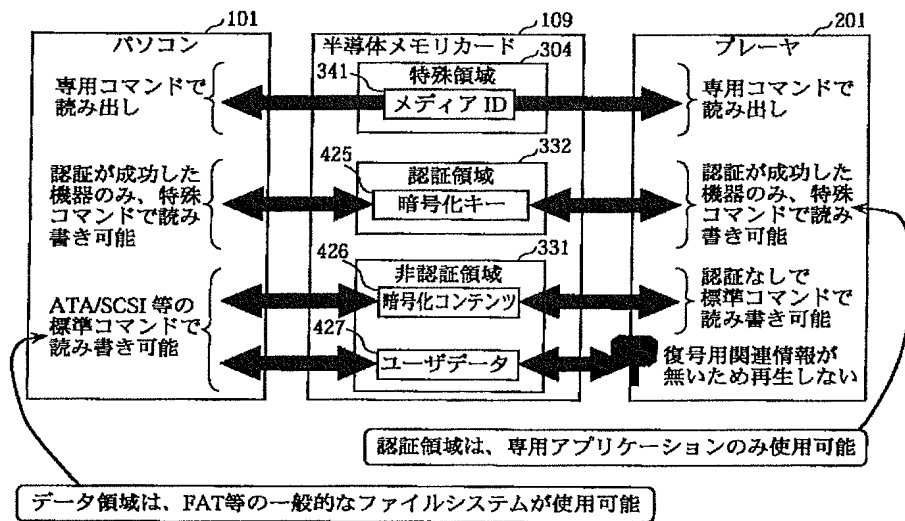
【符号の説明】

101	通信回線	10	219	D/Aコンバータ
102	PC		220	AACエンコーダ
103	ディスプレイ		221	A/Dコンバータ
104	キーボード		222	スクランブラ
105	メモリカードライタ挿入口		223	アナログ入力端子
106	スピーカ		224	スピーカ
107	メモリカードライタ		302	コントロールIC
108	メモリカード挿入口		303	フラッシュメモリ
109	メモリカード		304	ROM(特殊領域)
110	CPU		321	認証部
111	ROM	20	322	コマンド判定制御部
112	RAM		323	マスター鍵記憶部
113	通信ポート		323a	マスター鍵
114	内部バス		323b	暗号化マスター鍵
117	デスクランブラ		324	特殊領域アクセス制御部
118	AACデコーダ		325	認証領域アクセス制御部
119	D/Aコンバータ		326	非認証領域アクセス制御部
120	ハードディスク		327	暗号・復号化回路
201	プレーヤ		331	非認証領域
202	操作ボタン		332	認証領域
203	液晶表示部	30	341	メディアID
204	アナログ出力端子		342	製造メーカー名
205	デジタル出力端子		343	セキュアメディアID
206	メモリカード挿入口		425	暗号化キー
208	ヘッドフォン		426	暗号化コンテンツ
210	CPU		427	ユーザデータ
211	ROM		501	代替ブロック領域
212	RAM		812	読み出し回数
213	通信ポート		913	デジタル出力許可回数
214	内部バス		1003	乱数発生器
215	カードI/F部	40	1004	セクタ
216	認証回路		1005	拡張領域
217	デスクランブラ		1006	ECデータ
218	AACデコーダ		1007	時変領域
			1101	変換テーブル
			1102	認証領域専用変換テーブル
			1103	非認証領域専用変換テーブル
			1203	未消去リスト
			1301	マスター鍵
			1302	機器固有ID
			1310	機器固有ID群記憶領域
			1311	ユーザキー記憶領域

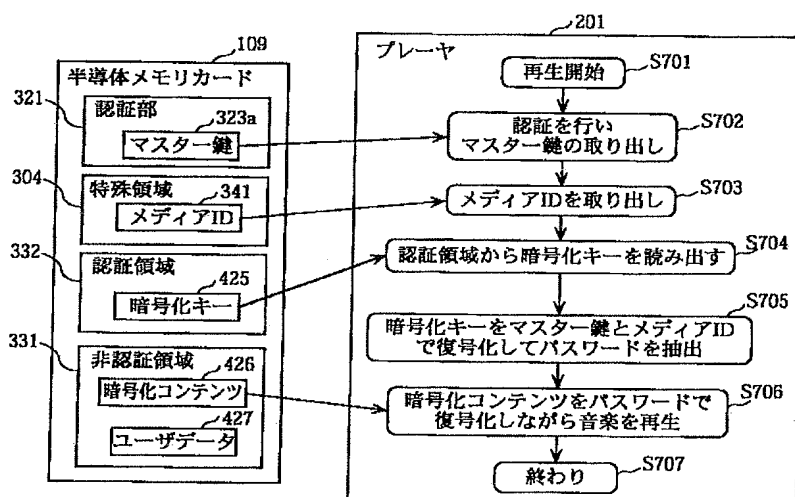
【図3】



【図6】



【図9】



【図10】

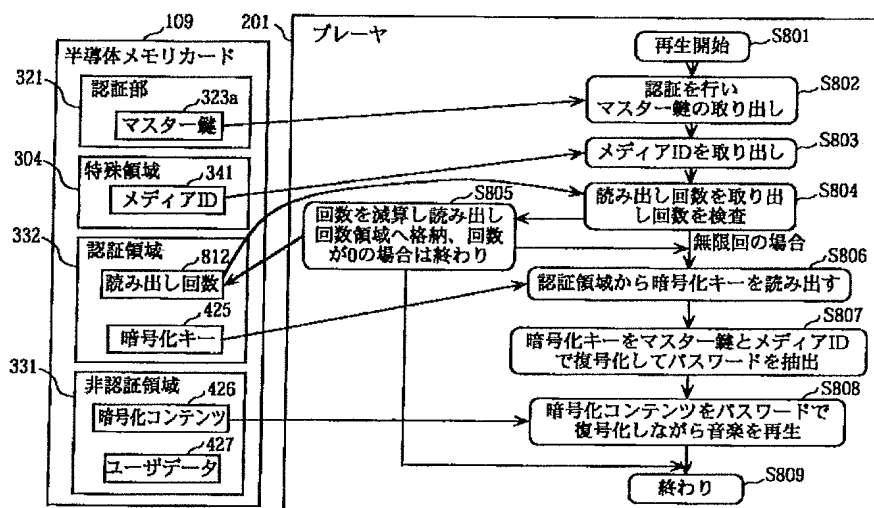
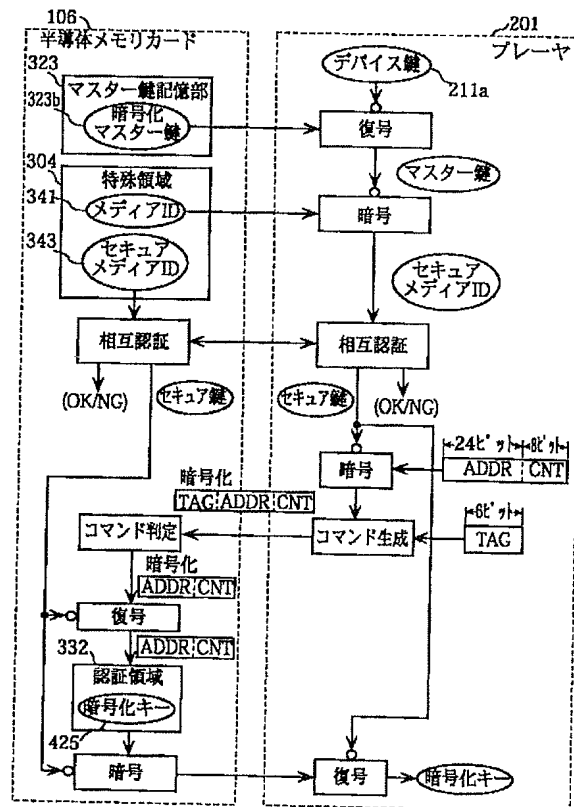
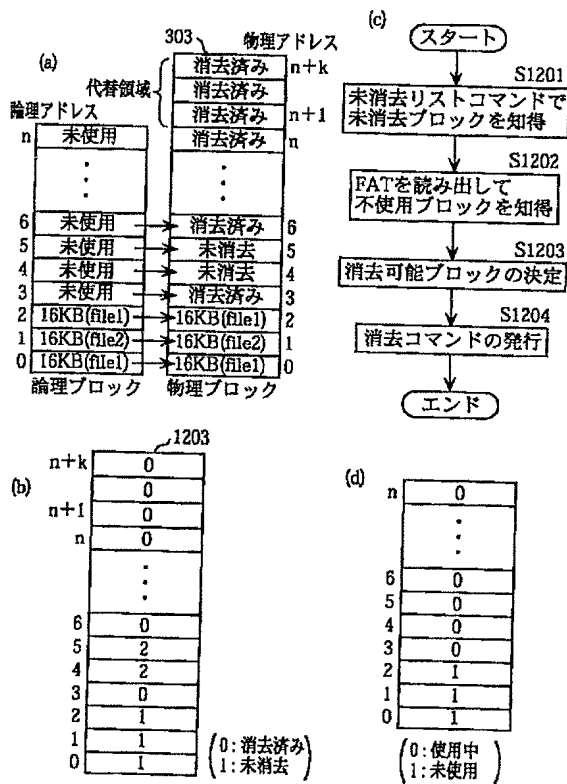


Figure 1 consists of four sub-diagrams labeled (a) through (d), illustrating address translation and mapping between logical and physical addresses.

- (a) Normal Mapping:** Shows a mapping from logical addresses (論理アドレス) to physical addresses (物理アドレス). A logical block (論理ブロック) is mapped to a physical block (物理ブロック) via a replacement area (代替領域). The mapping is shown for logical addresses 0, 1, 2, ..., n, n+1, ..., n+k. The physical addresses are 16KB(file1), 16KB(file2), ..., 16KB(file1).
- (b) Discontinuous Mapping:** Shows a mapping where a logical block (論理ブロック) is mapped to a physical block (物理ブロック) in a different file, indicating a discontinuity. The mapping is shown for logical addresses 0, 1, 2, ..., n, n+1, ..., n+k. The physical addresses are 16KB(file1), 16KB(file2), ..., 16KB(file1).
- (c) Continuous Mapping:** Shows a mapping where the physical address is replaced by the logical address, indicating a continuity area (連続領域). The mapping is shown for logical addresses 0, 1, 2, ..., n, n+1, ..., n+k. The physical addresses are 16KB(file1), 16KB(file2), ..., 16KB(file1).
- (d) Discontinuous Mapping:** Shows a mapping where the physical address is replaced by the logical address, indicating a discontinuity. The mapping is shown for logical addresses 0, 1, 2, ..., n, n+1, ..., n+k. The physical addresses are 16KB(file1), 16KB(file2), ..., 16KB(file1).

【図 16】



F ターム(参考) 5B017 AA07 BA05 BA07 BB02 BB10
CA14
5B035 AA06 AA13 BB09 BC00 CA07
CA11 CA38
5B058 CA25 CA27 KA02 KA06 KA35
YA16
5J104 AA07 KA02 NA02 NA05 NA33
NA35 NA41 PA14